National Infrastructure Protection Center CyberNotes

Issue #2002-22 *November 4, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 9 and between October 31, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acuma Software Limited[1]	Windows	Acusend 4.0	A vulnerability exists when a specially crafted URL request is sent, which could let an authenticated remote malicious user obtain sensitive information.	This issue is reportedly fixed in the most recent version of the software. Users should contact the vendor at: http://www.acumasoftware.co.uk	Acusend Unauthorized File Access	Medium	Bug discussed in newsgroups and websites.

[1] Sec-Tec Advisory 24.10.02, October 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alt-N Technologies, LTD[2]	Multiple	MDaemon 6.0.0, 6.0.5-6.0.7	A buffer overflow vulnerability exists in some POP server commands due to inadequate bounds checking, which could let a malicious user cause a Denial of Service.	Upgrade available at: http://www.altn.com/Products/Default.asp?product_id=MDaemon	MDaemon POP Server Buffer Overflow	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
America OnLine[3]	Windows	Instant Messenger 4.8.2790	A vulnerability exists because it is possible to send a malicious link that points to an executable file, which could let a malicious user execute arbitrary files on the client system.	Upgrade or downgrade to another version.	AOL Instant Messenger Local File Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
AN-HTTPd[4]	Windows 95/98/ME NT 4.0/2000, XP	AN-HTTPd 1.41 d	A Cross-Site Scripting vulnerability exists because HTML tags are not properly filtered from URL parameters, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://www.st.rim.or.jp/~nakata/httpd141e.exe	AN-HTTPD Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
AN-HTTPd[5]	Windows 95/98/ME/ NT 4.0/2000, XP	AN-HTTPd 1.38-140, 1.41, 1.41b, 1.41	A buffer overflow vulnerability exists due to insufficient bounds checking of usernames in SOCKS4, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.st.rim.or.jp/~nakata/httpd141d.zip	AN HTTPD Malformed SOCKS4 Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Apple Computer, Inc.[6]	MacOs	12/640 Laser Writer TCP/IP Configuration Utility	A vulnerability exists because Telnet access has no password set, which could let a remote malicious user obtain unauthorized access to the device.	No workaround or patch available at time of publishing.	12/640 PS LaserWriter TCP/IP Telnet Server Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Arescom[7]	Multiple	NetDSL-800	A vulnerability exists because it is possible to obtain an undocumented username and password for target devices using a network sniffer and the NetDSL Remote Manager, which could let a remote malicious user corrupt configuration settings or cause a Denial of Service.	No workaround or patch available at time of publishing.	NetDSL-800 Firmware Undocumented Username/ Password Weakness	Low/ Medium (Medium if configuration settings can be corrupted)	Bug discussed in newsgroups and websites.

[2] Bugtraq, October 27, 2002.
[3] Bugtraq. October 21, 2002.
[4] SNS Advisory No.57, October 28, 2002.
[5] Securiteam, October 21, 2002.
[6] UkR Security Team, October 26, 2002.
[7] Bugtraq, October 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Balabit[8, 9] ***Engarde releases new patches and SuSE releases patches[10, 11]***	**Unix**	**syslog-ng 1.4 .0rc3, 1.4.7-1.4.10, 1.4.15, 1.5.15, 1.5.20**	**A buffer overflow vulnerability exists because the syslog-ng macro expansion fails to do proper bounds checking when handling constant characters, which could let a remote malicious user execute arbitrary commands.**	**Debian:** **http://security.debian.org/pool/updates/main/s/syslog-ng/** **Engarde:** **ftp://ftp.engardelinux.org/pub/engarde/stable/updates/** **Balabit:** **http://www.balabit.hu/en/downloads/syslog-ng/downloads/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**Syslog-ng Remote Buffer Overflow** **CVE Name: CAN-2002-1200**	**High**	**Bug discussed in newsgroups and websites.**
Benjamin Lefevre[12]	Unix	Dobermann FORUM 0.1-0.5	A vulnerability exists in several of the PHP script files, which could let a remote malicious user include arbitrary files located on remote servers.	No workaround or patch available at time of publishing.	Dobermann Forum Remote File Include	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
BRS[13]	Windows NT	Web Weaver 1.01	A vulnerability exists because it is possible to bypass input validation, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebWeaver Web Server File Access	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[8] Debian Security Advisory, DSA 175-1, October 15, 2002.
[9] EnGarde Secure Linux Security Advisory, ESA-20021016-025, October 16, 2002.
[10] EnGarde Secure Linux Security Advisory, ESA-20021029-028, October 29, 2002.
[11] SuSE Security Announcement, SuSE-SA:2002:039, October 31, 2002.
[12] Bugtraq, October 27, 2002.
[13] Bugtraq, October 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
bzip2[14]	Unix	bzip2 0.9.5a-0.9.5d, 0.9.0-0.9.0c,1.0, 1.0.1	Multiple vulnerabilities exist: a vulnerability exists because the O_EXCL flag is not used to create files during decompression and the user is not warned if an existing file would be overwritten, which could allow a malicious user to overwrite files via a bzip2 archive; a vulnerability exists because files are decompressed with world-readable permissions before setting the permissions to what is specified in the bzip2 archive, which could let a malicious user read files as they are being decompressed; and a vulnerability exists because permissions of symbolic links are used when creating an archive instead of the actual files, which could cause the files to be extracted with less restrictive permissions than intended.	Upgrade available at: http://sources.redhat.com/bzip2/index.html#bzip2-latest **SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/	bzip2 Multiple Vulnerabilities CVE Name: CAN-2002-0759	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Caldera International, Inc. [15]	Unix	OpenUnix 8.0; UnixWare 7.1.1	A Denial of Service vulnerability exists in the RPC program when the /proc file system is copied.	Patch available at: ftp://ftp.sco.com/pub/updates/OpenUNIX/CSSA-2002-SCO.41/erg712112c.pkg.Z	UnixWare/ OpenUnix Proc File System Denial of Service CVE Name: CAN-2002-1231	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[14] SCO Security Advisory, CSSA-2002-039.0, October 29, 2002.

[15] SCO Security Advisory, CSSA-2002-SCO.41, October 21, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[16]	Multiple	ONS 15327 3.0-3.3, ONS 15454 Optical Transport Platform 3.0, 3.1 .0, 3.2 .0, 3.3	Multiple vulnerabilities exist: a vulnerability exists because it is possible to open a FTP connection to the TCC, TCC+ or XTC using any nonexistent user-name and password, which could let a malicious user upload modified configuration files and delete software images; a vulnerability exists because user-names and passwords are stored in clear text in the running image database, which could let a local/remote malicious user obtain complete control over the ONS platform; a vulnerability exists because the SNMP community string "public" cannot be changed in the ONS software, which could let a malicious obtain unauthorized access; a vulnerability exists when a malicious user requests an invalid CORBA Interoperable Object Reference (IOR) via HTTP which would cause the TCC, TCC+ or XTC to reset; a vulnerability exists when a malicious user sends a HTTP request that starts with any character other than '/' which may cause the TCC, TCC+, TCCi or XTC to reset; and a vulnerability exists because the TCC, TCC+ and XTC have a user-name and password that can be used to gain access to the underlying VxWorks Operating System and it is not possible to change or disable this account, which could let a local/remote malicious user obtain complete control over the ONS platform.	The procedure to upgrade to the fixed software version on the Cisco ONS 15454 is detailed at: http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r34dohcs/procedur/r34pctc.htm. The procedure to upgrade to the fixed software version on the Cisco ONS 15327 is detailed at: http://www.cisco.com/univercd/cc/td/doc/product/ong/15327/r34userd/2734ctc.htm	Cisco ONS15454/ONS15327 Optical Transport Platforms Multiple Vulnerabilities	Medium/ **High** **(High if complete control can be obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Darren Reed[17]	Unix	IPFilter 3.1.1-3.1.10, 3.2.1-3.2.22, 3.3.1-3.3.22, 3.4.1-3.4.28	A vulnerability exists because under certain circumstances ports can be opened on FTP servers, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://coombs.anu.edu.au/~avalon/ip-fil3.4.29.tar.gz	IPFilter FTP Proxy Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[16] Cisco Security Advisory, 20021031, October 31, 2002.
[17] SecurityFocus, October 19, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
D-Link[18]	Multiple	DSL-500	A vulnerability exists because the default Telnet password can't be changed, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	DSL-500 Default Telnet Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
D-Link[19]	Multiple	DWL-900AP+ 2.1, 2.2	A vulnerability exists in the TFTP server which could let a remote malicious user obtain sensitive information and potentially full administrative access.	No workaround or patch available at time of publishing.	DWL-900AP+ TFTP Server	Medium/ **High** **(High if adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Dug Song[20]	Unix	Fragrouter 1.7	A vulnerability exists because the server hosting fragrouter, www.anzen.com, was compromised and modifications were made to the source code to include Trojan horse code. Downloads of the fragrouter source code from www.anzen.com between October 18, 2002 and October 19, 2002 likely contain the Trojan code. The modified version was placed on the Web site as fragrouter-1.7.tar.gz. This vulnerability could result in a complete system compromise for the affected users.	Users that require fragrouter use either a known good version of fragrouter 1.6, or the fragroute package, which is currently maintained.	Fragrouter Trojan Horse	**High**	Bug discussed in newsgroups and websites. The source code of the Trojan horse has been made published.
FlashFXP[21]	Windows	FlashFXP 1.4	A vulnerability exists because plaintext passwords for FTP sites can be viewed when file transfers exist in the queue, which could let a malicious user obtain sensitive information and unauthorized access.	Upgrade available at: http://www.flashfxp.com/	FlashFXP Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[18] Bugtraq, October 23, 2002.
[19] ETHEREANET-NCC Security Report EN-NCC-20021014-04, October 21, 2002.
[20] VulnWatch, October 21, 2002.
[21] Bugtraq, October 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ghost View[22] ***Patches are released[23, 24, 25, 26, 27, 28, 29, 30]***	**Unix**	**GhostView 1.3, 1.4, 1.4.1, 1.5, gv 2.7 b1-b5, 2.7.6, 2.9.4, 3.0.0, 3.0.4, 3.1.4, 3.1.6, 3.2.4, 3.4.2, 3.4.3, 3.4.12, 3.5.2, 3.5.3, 3.5.8**	**A buffer overflow vulnerability exists in the sscanf() function when a malformed postscript or Adobe pdf file is sent, which could let a malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.** ***Debian:*** **http://security.debian.org/pool/updates/main/g/gnome-gv/** http://security.debian.org/pool/updates/main/k/kdegraphics ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com/** ***KDE:*** **ftp://ftp.kde.org/pub/kde/security_patches/post-2.2.2-kdegraphics-kghostview.diff**	**GhostView Buffer Overflow** **CVE Name: CAN-2002-0838**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
GNU[31] ***More patches released[32]***	**Unix**	**SharUtils 4.2; Caldera OpenLinux Server 3.1, 3.1.1, OpenLinux Works-tation 3.1, 3.1.1**	**A vulnerability exists because uudecode does not check for the existence of the file before it is created from the decoded archive, which could let a malicious user overwrite arbitrary files or obtain escalated privileges.**	**Update available at:** **ftp://updates.redhat.com/** **SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/ **RedHat:** ftp://updates.redhat.com/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	**SharUtils UUDecode Symbolic Link Attack** **CVE Name: CAN-2002-0178**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
GTetrinet[33]	Multiple	GTetrinet 0.4-0.4.3	Several buffer overflow vulnerabilities exist due to insufficient bounds checking. which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.	Update available at: http://download.sourceforge.net/gtetrinet/gtetrinet-0.4.4.tar.gz	GTetrinet Multiple Remote Buffer Overflow Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Hans Persson[34]	Unix	Molly 0.5	A vulnerability exists due to the improper validation of user-supplied input in the &host variable, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Molly Host Execute Commands	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[22] iDEFENSE Security Advisory, 09.26.2002, September 26, 2002.
[23] Gentoo Linux Security Announcement, 200210-003, October 17, 2002.
[24] Debian Security Advisory, DSA 176-1, October 16, 2002.
[25] Debian Security Advisory, DSA 179-1, October 18, 2002.
[26] Debian Security Advisory, DSA 182-1, October 28, 2002.
[27] Mandrake Linux Security Update Advisory, MDKSA-2002:069, October 22, 2002.
[28] Mandrake Linux Security Update Advisory, MDKSA-2002:071, October 24, 2002.
[29] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:212-06, October 4, 2002.
[30] KDE Security Advisory, October 9, 2002.
[31] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:065-13, May 14, 2002.
[32] Gentoo Linux Security Announcement, 200210-012, October 30, 2002.
[33] SecurityFocus, October 30, 2002.
[34] SCAN Associates Advisory, October 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[35]	Multiple	Infoprint Controller Software 1.0 47012	A buffer overflow vulnerability exists in the Telnet based remote management services due to insufficient checks on user-supplied input for the login parameter, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Infoprint Printers Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM[36]	Windows 2000, Unix	WebSphere Caching Proxy Server 3.6, 4.0	A remote Denial of Service vulnerability exists in the Caching Proxy component due to inadequate checks when HTTP headers are processed.	Users are advised to install Caching Proxy efix build 4.0.1.26. Users of Caching Proxy Server 3.6 are advised to contact their vendor for information about obtaining fixes.	Websphere Caching Proxy Remote Denial of Service CVE Name: CAN-2002-1169	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IBM[37]	Windows NT 4.0/2000, Unix	WebSphere Caching Proxy Server 3.6, 4.0	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in the web caching component due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	Users of Caching Proxy Server 3.6 are advised to contact their vendor for information about obtaining fixes.	IBM Websphere Vulnerabilities CVE Names: CAN-2002-1167, CAN-2002-1168	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
IPSwitch, Inc.[38]	Windows	WS FTP Server 3.1.3	Two vulnerabilities exist: a FTP bounce vulnerability exists when a specially crafted FTP command is submitted, which could let a remote malicious user send arbitrary data to other systems; and a PASV connection hijacking vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WS_FTP Server FTP Bounce and PASV Connection Hijacking	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[35] Securiteam, October 25, 2002.
[36] Rapid 7, Inc. Security Advisory, R7-0007, October 23, 2002.
[37] Rapid 7, Inc. Security Advisory, R7-0008, October 23, 2002.
[38] Securiteam, October 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ISC[39]	Unix	INN 2.0-2.2.3; SCO OpenLinux 3.1.1 Server, 3.1 Server	Multiple vulnerabilities exist in the 'inews' and 'rnews' components due to insecure open() calls in some of the binaries and format string vulnerabilities, which could let a malicious user replace/Trojan other system files or obtain sensitive information.	Upgrade available at: ftp://ftp.isc.org/isc/inn/inn-2.3.3.tar.gz **SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/	INN Multiple Insecure Open Call CVE Name: CAN-2002-0526	Medium	Bug discussed in newsgroups and websites.
Jelsoft Enter-prises[40]	Windows, Unix	VBulletin 2.0 rc3, rc2, 2.2.0-2.2.8	A Cross-Site Scripting vulnerability exists in the 'usercp.php' script because URI parameters are not properly filtered from HTML tags, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.vbulletin.com/forum/showthread.php?threadid=57203	VBulletin Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
kmMail[41]	Unix	kmMail 1.0 b & prior	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of HTML and script code from the body of e-mail messages, which could let a malicious user execute arbitrary HTML and script code.	Upgrade available at: http://prdownloads.sourceforge.net/kmmail/kmmail-1.0b.1.tar.gz?download	kmMail E-Mail Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Linksys[42]	Multiple	WET11 Wireless Ethernet Bridge	A remote Denial of Service vulnerability exists when a malicious user sends an Ethernet frame containing the affected device's MAC address in the DLC header.	No workaround or patch available at time of publishing.	WET11 Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Mail-reader.com[43]	Unix	Mailreader.com 2.3.20-2.3.31	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists which could let al remote malicious user obtain sensitive information; and a vulnerability exists in versions 2.3.30-2.2.31 because user-supplied input is not properly sanitized of shell metacharacters before it is passed to the sendmail MTA, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.mailreader.com/download/mailreader-2.3.33.tar.gz	MailReader.com Directory Traversal & Remote Command Execution	Medium/ **High** **(High if arbitrary can be executed)**	Bug discussed in newsgroups and websites. Vulnerabilities can be exploited via a web browser.

[39] SCO Security Advisory, CSSA-2002-038.0, October 24, 2002.
[40] Bugtraq, October 18, 2002.
[41] Securiteam, October 21, 2002.
[42] enZo Notice, October 24, 2002.
[43] SCAN Associates Advisory, October 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mark Ruef[44]	Unix	Virgil CGI Scanner 0.9	A vulnerability exists due to a failure to properly sanitize user-supplied input, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Virgil CGI Scanner Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Martin Bauer[45]	Windows, Unix	gBook 1.4	A vulnerability exists in the 'index.php' script, which could let an unauthorized remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	gBook Administrative Access	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[46]	Windows 2000	Windows 2000 Advanced Server, SP1&2, 2000 Datacenter Server, SP1&2, 2000 Profes-sional, SP1&2, 2000 Server, SP1&2, 2000 Terminal Services, SP1&2	A Denial of Service vulnerability exists in 'snmp.exe' due to a memory leak when a large number of SNMP queries are sent to obtain print queue information.	Upgrade to Windows 2000 Service Pack 3 available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/sp3lang.asp	Microsoft Windows 2000 SNMP Printer Query Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited using any SNMP management utility.
Microsoft[47]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0	A vulnerability exists due to lack of control checks when a document object is accessed through a saved reference, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Document. Write() Zone Bypass	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[48]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	Multiple vulnerabilities exist due to the way cached objects are handled and the lack of access control checks when a document object is accessed through a separate reference, which could let a remote malicious user execute arbitrary code.	Upgrade to Internet Explorer 6.0 with Service Pack 1 available at: http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/default.asp	Multiple Microsoft Internet Explorer Cached Objects Zone Bypass	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[44] KALIF Research Group, October 21, 2002.
[45] Bugtraq, October 22, 2002.
[46] Securiteam, October 22, 2002.
[47] Bugtraq, October 21, 2002.
[48] GreyMagic Security Advisory GM#012-IE, October 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[49]	Windows, Unix	Windows Media Player 6.3 Solaris	A vulnerability exists because executables are installed with world-writeable permissions, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Windows Media Player World Writeable Executables	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[50]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a	A vulnerability exists due to the way Windows NT and 2000 searches for an application when the path is not specified, which could let a malicious user mount a Trojan horse attack.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-064.asp	Microsoft Windows 2000 / NT Path Precedence CVE Name: CAN-2002-1184	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[51]	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, 2000 SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A remote Denial of Service vulnerability exists in the Remote Procedure Call (RPC) Service when a specifically malformed packet is sent to TCP port 135.	No workaround or patch available at time of publishing.	Windows 2000 RPC Service Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.

[49] Bugtraq, October 18, 2002.
[50] Microsoft Security Bulletin, MS02-064, October 30, 2002.
[51] Immunity Inc. Advisory, October 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[52]	Windows NT 4.0/2000, XP	Internet Information Service (IIS) 4.0, 5.0, 5.1	Multiple vulnerabilities exist: a vulnerability exists due to the way ISAPIs are launched when configured to run out of process, which could let a malicious user obtain elevated privileges; a Denial of Service vulnerability exists due to the way memory is allocated for WebDAV requests; a vulnerability exists that involves the operation of the script source access permissions in IIS 5.0, which could let a malicious user with write access upload an arbitrary file and execute it; and a pair of Cross-Site Scripting vulnerabilities exist that involve administrative web pages due to improper sanitization of user-supplied input, which could let a malicious user execute arbitrary HTML and script code.	Frequently asked questions regarding this vulnerability and the patches can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-062.asp	Internet Information Service Vulnerabilities CVE Names: CAN-2002-0869, CAN-2002-1180, CAN-2002-1181, CAN-2002-1182	Low/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for these vulnerabilities.
Microsoft[53]	Windows 2000, XP	2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A security vulnerability exists in the Windows 2000 and Windows XP implementations because of an unchecked buffer in a section of code that processes the control data used to establish, maintain, and tear down PPTP connections, which could let a malicious user cause a Denial of Service. and possibly execute arbitrary code.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-063.asp	Microsoft PPTP Buffer Overrun CVE Name: CAN-2002-1214	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[52] Microsoft Security Bulletin, MS02-062, October 30, 2002.
[53] Microsoft Security Bulletin, MS02-063, October 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mojo Mail[54]	Unix	Mojo Mail 2.7	A Cross-Site Scripting vulnerability exists because URI parameters are not properly filtered from HTML tags, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Mojo Mail Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Multiple Vendors[55]	Unix	Apache Software Foundation Apache 2.0, 2.0.35-2.0.42; HP HP-UX 11.0, 11.11, 11.20, 11.22	A vulnerability exists when WebDAV and CGI are enabled for folders due to inadequate checks on CGI scripts, which could let a remote malicious user obtain sensitive information.	Customers of HP-UX are advised to download Apache 2.0.43.00 product bundles available at: http://www.software.hp.com/ISS_products_list.html **Apache Software Foundation:** http://www.apache.org/dist/httpd/	Apache 2 WebDAV CGI Information Disclosure CVE Name: CAN-2002-1156	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[56]	Multiple	NetScreen ScreenOS 2.7.1, 2.7.1 r1-r3, 2.10 r3&r4, 3.0.1 r1&r2, 3.0.3 r1.1	A remote Denial of Service vulnerability exists because certain types of input are not properly handled.	NetScreen has acknowledged that some of their product line is affected. Users should contact the vendor for further details.	Multiple Firewall Vendor Packet Flood State Table Filling Remote Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited using any number of packet flooding utilities available.

[54] Securiteam, October 25, 2002.
[55] Hewlett-Packard Company Security Bulletin, HPSBUX0210-224, October 30, 2002.
[56] SecurityFocus, October 21, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[57]	Unix	Apple MacOS X 10.2 (Jaguar), MacOS X Server 10.2; FreeBSD FreeBSD 4.6, 4.6 – STABLE, RELEASE; FreeS/ WAN FreeS/ WAN 1.9-1.9.6; Global Technology Associates GNAT Box Firmware 3.1-3.3; NEC BlueFire IX1035, NEC IX1010, IX1011, IX1020, IX1050, IX2010; NetBSD NetBSD 1.5, 1.5 x86, sh3, 1.5.1-1.5.3, 1.6 beta	A vulnerability exists in several implementations of IPSec due to the way malformed ESP packets are handled because authentication header data is improperly validated, which could let a remote malicious user cause a Denial of Service.	Patches for eSoft's InstaGate are available via SoftPak Director. **Internet Initiative Japan:** Upgrade to a firmware revision greater than version 1.63 available at: http://www.seil-neu.com/ **Apple:** http://download.info.apple.com/Mac_OS_X/ **FreeBSD:** http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet6/esp_input.c#rev1.1.2.7 **Global Technology Associates GNAT Box:** http://www.gta.com/support/center/	Multiple Vendor IPSec Implementation Denial of Service CVE Name: CAN-2002-0666	Low	Bug discussed in newsgroups and websites.

[57] NetBSD Security Advisory, 2002-016, October 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[58] [59] *More patches released*[60], [61], [62], [63], [64] *Proof of Concept exploit has been published.*[65] *HP releases bulletin*[66]	Windows NT 4.0/2000, Unix	Apache Software Foundation Apache 1.3.20, 1.3.22-1.3.26; Oracle Internet Application Server 1.0.2.1, 1.0.2.0, 8i Enterprise Edition 8.1.7.1.0, 8.1.7.0.0, 9i Application Server, 1.0.2.2, 1.0.2.1s, 1.0.2, 9.0.2, 9.0.2 release 2, 9iAS Reports 9.0.2 .1, Oracle8 8.1.7, 8.1.7.1, 8.1.7, Oracle9i Release 2 9.2 .2, 9.0.2	Multiple vulnerabilities exist: a Denial of Service vulnerability exists due to the way the Apache scorecare is handled; a Cross-Site Scripting vulnerability exists due to improper sanitization of SSI error pages, which could let a malicious user execute arbitrary HTML or JavaScript code; and a buffer overflow vulnerability exists in the ab.c web benchmarking support utility, which could let a malicious user execute arbitrary code.	Apache Software Foundation: http://www.apache.org/dist/httpd/apache_1.3.27.tar.gz Oracle Corporation: Oracle has stated that fixes for affected software will be available October 8, 2002 through metalink. *OpenPKG:* ftp://ftp.openpkg.org/release/1.0/UPD/ *Engarde Secure Linux:* ftp://ftp.engardelinux.org/pub/engarde/stable/updates/i386/apache-1.3.27-1.0.32.i386.rpm *Mandrake:* http://www.mandrakesecure.net/en/ftp.php FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/All/ Oracle: http://metalink.oracle.com *Trustix:* http://www.trustix.net/pub/Trustix/updates/ *The fixes for all HP-UX versions are in the form of new product bundles, instead of patches available at:* *http://www.software.hp.com/ISS_products_list.html*	Apache Web Server Multiple Vulnerabilities CVE Names: CAN-2002-0839, CAN-2002-0840, CAN-2002-0843	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. *Proof of Concept exploit has been published for the Cross-Site Scripting Vulnerability.*

[58] iDEFENSE Security Advisor, 10.03.2002, October 3, 2002.
[59] OpenPKG Security Advisory, OpenPKG-SA-2002.009, October 4, 2002.
[60] EnGarde Secure Linux Security Advisory, ESA-20021007-024, October 7, 2002.
[61] FreeBSD Security Notice, FreeBSD-SN-02:06, October 10, 2002.
[62] Mandrake Linux Security Update Advisory, MDKSA-2002:068, October 16, 2002.
[63] Oracle Security Alert #45, October 4, 2002.
[64] Trustix Secure Linux Security Advisory, 2002-0069, October 17, 2002.
[65] SecurityFocus, October 30, 2002.
[66] Hewlett-Packard Company Security Bulletin, HPSBUX0210-224, October 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[67] [68, 69] *SCO releases patch*[70]	Unix	HP Secure OS software for Linux 1.0; Mandrake Soft Corporate Server 1.0.1, Mandrake 7.0, 7.1, 7.2, 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2, Single Network Firewall 7.2; RedHat Linux 6.0, 6.0 sparc, alpha, 6.1, 6.1 sparc, alpha, 6.2, 6.2 sparc, alpha, 7.0, 7.0 alpha, 7.1, 7.1 ia64, alpha, 7.2, 7.2 ia64, alpha, 7.3; Sun Cobalt RaQ-RaQ 5, RaQ XTR, Cache RaQ series, Qube-Qube3, Control Station	A vulnerability exists in the 'chfn' utility due to the failure to check the existence of a lockfile prior to performing sensitive operations, which could let a malicious user inject arbitrary data into these files to obtain elevated privileges.	RedHat: ftp://updates.redhat.com/ Trustix: http://www.trustix.net/pub/Trustix/updates/ *SCO:* ftp://ftp.sco.com/pub/updates/OpenLinux/	Util-linux File Locking Race Condition CVE Name: CAN-2002-0638	Medium	Bug discussed in newsgroups and websites.

[67] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:132-14, July 29, 2002.
[68] Trustix Secure Linux Security Advisory, TSLSA-2002-0064, July 30, 2002.
[69] Hewlett-Packard Company Security, HPSBTL0207-054, July 30, 2002.
[70] SCO Security Advisory, CSSA-2002-043.0, October 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[71, 72, 73, 74]	Unix	Debian Linux 2.2, 2.2 sparc, powerpc, IA-32, alpha, arm, 68k, 3.0, 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, happa, arm, alpha; HP Secure OS software for Linux 1.0; RedHat 6.2, 6.2 sparc, i386, alpha, 7.0, 7.0 i386, alpha, 7.1, 7.1 ia64, i386, 7.2, 7.2 ia64, 7.3, 7.3 i386	A vulnerability exists in the 'ypserv' daemon when a malicious Network Information Service (NIS) request is issued, which could let a remote malicious user obtain sensitive information.	**Debian:** http://security.debian.org/pool/updates/main/n/nis/ **RedHat:** ftp://updates.redhat.com/	YPServ Remote Network Information Leakage CVE Name: CAN-2002-1232	Medium	Bug discussed in newsgroups and websites.

[71] Debian Security Advisory, DSA 180-1, October 21, 2002.
[72] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:223-07, October 24, 2002.
[73] Hewlett Packard Security Bulletin, HPSBTL0210-074, October 26, 2002.
[74] Gentoo Linux Security Announcement, 200210-010, October 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[75, 76, 77, 78, 79]	Unix	EnGarde Secure Linux 1.0.1; Mandrake Soft Linux Mandrake 7.2, 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2, 8.2 ppc, 9.0, Single Network Firewall 7.2; mod_ssl mod_ssl 2.4.10, 2.8.9; OpenPKG OpenPKG Current, 1.0, 1.1	A Cross-Site Scripting vulnerability exists in mod_ssl where, under certain circumstances, Apache will use the client supplied hostname:port pair, which could let a remote malicious user execute arbitrary HTML and script code. *Note: Existence of this vulnerability is limited to configurations with both the 'UseCanonicalName' option turned off and wildcard DNS enabled.*	**EnGarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/i386/apache-1.3.27-1.0.33.i386.rpm **Mandrake:** ftp://ftp.planetmirror.com/pub/Mandrake/updates **OpenPKG:** ftp://ftp.openpkg.org/	Mod_SSL Cross-Site Scripting CVE Name: CAN-2002-1157	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[80, 81, 82, 83, 84, 85, 86, 87]	Unix	KTH eBones 1.2, Heimdal 0.3 e, 0.4 a-0.4 e, 0.5, 0.21; MIT Kerberos 4 1.0, 1.1, 4.0, Kerberos 5 1.0, 1.0.6, 1.1, 1.1.1, 1.2-1.2.6; NetBSD NetBSD 1.5-1.5.3, 1.6; OpenBSD OpenBSD 3.0, 3.1	A buffer overflow vulnerability exists in the 'kadmind' daemon due to insufficient bounds checking, which could let a remote malicious user obtain root privileges and execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/h/heimdal/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **MIT Kerberos:** http://web.mit.edu/kerberos/www/advisories/2002-002-kadm4_patch.txt **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patchees/ **NetBSD:** ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-026.txt.asc	Multiple Vendor kadmind Remote Buffer Overflow CVE Name: CAN-2002-1235	**High**	Bug discussed in newsgroups and websites. Exploit is circulating in the wild. Vulnerability has appeared in the press and other public media.

[75] EnGarde Secure Linux Security Advisory, ESA-20021029-027, October 29, 2002.
[76] Debian Security Advisory, DSA 181-1, October 22, 2002.
[77] OpenPKG Security Advisory, OpenPKG-SA-2002.010, October 23, 2002.
[78] Mandrake Linux Security Update Advisory, MDKSA-2002:072, October 24, 2002.
[79] Gentoo Linux Security Announcement, 200210-009, October 27, 2002.
[80] NetBSD Security Advisory, 2002-026, October 21, 2002.
[81] Gentoo Linux Security Announcement, 200210-008, October 26, 2002.
[82] CERT Advisory, CA-2002-29, October 25, 2002.
[83] Debian Security Advisory, DSA 183-1, October 29, 2002.
[84] Debian Security Advisory ,DSA 184-1, October 30, 2002.
[85] Mandrake Linux Security Update Advisory, MDKSA-2002:073, October 29, 2002.
[86] MIT krb5 Security Advisory, MITKRB5-SA-2002-, October 26, 2002.
[87] NetBSD Security Advisory, 2002-026, October 21, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MyMarket[88]	Unix	MyMarket 1.71	A Cross-Site Scripting vulnerability exists in the 'form_header.php' script because HTML tags and script code are note properly sanitized from CGI variables, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	MyMarket Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
NetBSD[89]	Unix	NetBSD 1.5-1.5.3, 1.6	A buffer overflow vulnerability exists in Trek because privileges are not dropped, which could let a malicious user obtain elevated privileges.	Upgrade available at:	NetBSD Trek Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Oracle Corporation[90]	Windows NT 4.0/2000, XP, Unix	Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists due to improper bounds checking of the USERID parameter, which could let a malicious user overwrite sensitive stack variables, in an effort to execute arbitrary code.	Patch available at: http://metalink.oracle.com	Oracle 9i Database Server Malformed USERID Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Perception Software[91]	Windows 98/2000	LiteServe 2.0	A vulnerability exists because it is possible to construct a web request that is capable of accessing the contents of password protected files/folders, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	LiteServe Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Perlbot[92]	Windows, Unix	Perlbot 1.9.2	Several vulnerabilities exist: a vulnerability exists due to improper filtering of user-supplied input when using the $filename variable, which could let a remote malicious user execute arbitrary commands; and a vulnerability exists due to improper filtering of user-supplied input when using the $text variable, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Perlbot Remote Command Execution Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Perlbot[93]	Windows, Unix	Perlbot 1.0 beta	A vulnerability exists due to improper filtering when the script sends an e-mail, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Perlbot E-mail Sending Remote Command Execution	**High**	Bug discussed in newsgroups and websites.

[88] Bugtraq, October 21, 2002.
[89] NetBSD Security Advisory, 2002-025, October 24, 2002.
[90] Oracle Security Alert #46, October 31, 2002.
[91] Bugtraq, October 24, 2002.
[92] SCAN Associates Advisory, October 18, 2002.
[93] SCAN Associates Advisory, October 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Perlbot[94]	Windows, Unix	Perlbot 1.0 beta	A vulnerability exists due to improper filtering of user-supplied input, which could let a remote malicious user execute shell commands.	No workaround or patch available at time of publishing.	Perlbot Arbitrary Shell Script	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP Arena[95]	Windows, Unix	paFileDB 1.1.3, 2.1.1	A Cross-Site Scripting vulnerability exists when JavaScript is used as a search string, which could let la remote malicious user execute arbitrary HTML or script code.	Upgrade available at: http://www.phparena.net/downloads/pafiledb.php?action=file&id=16	paFileDB Search Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP Arena[96]	Windows, Unix	paFileDB 1.1.3, 2.1.1, 3.0	Several Cross-Site Scripting vulnerabilities exist: a vulnerability exists in the “Email to Friend” function, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the "Download" function, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in the “Rate” function, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	paFileDB Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
phpBB Group[97]	Unix	phpBB 2.0.0	A vulnerability exists in the ‘admin_ug_auth.php’ script, which could let an unauthorized malicious user obtain administrative privileges.	Upgrade available at: http://www.phpbb.com/downloads.php	phpBB2 Unauthorized Administrative Access	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
RadioBird Software[98]	Windows NT	WebServer 4 All 1.28	A buffer overflow vulnerability exists in the ‘Host.’ HTTP header field due to inadequate bounds checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: ftp://ftp.freeware.lt/anonymous/Soft/w4asetup.exe	WebServer 4 All Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[94] SCAN Associates Advisory, October 18, 2002.
[95] Bugtraq, October 20, 2002.
[96] Bugtraq, October 20, 2002.
[97] Bugtraq, October 27, 2002.
[98] Bugtraq, October 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Software 602[99]	Windows 98/ME/NT 4.0/2000, XP	602Pro LAN SUITE 2002	A vulnerability exists in the '/admin/' folder because access can be obtained without authorization, which could let a malicious user perform unauthorized administrative actions.	No workaround or patch available at time of publishing.	Web602 Unauthorized Admin Directory Access	**High**	Bug discussed in newsgroups and websites.
Solar Winds[100]	Windows	TFTP Server Standard Edition 5.0.55	A Denial of Service vulnerability exists when a malicious user sends an UDP packet to the server that is 8193 or more bytes.	No workaround or patch available at time of publishing.	TFTP Server Large UDP Packet Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Solar Winds[101]	Windows	TFTP Server Standard Edition 5.0.55	A Directory Traversal vulnerability exists because user-supplied input is not properly handled, which could let a remote malicious user obtain sensitive information.	Upgrade available at: ftp://ftp.solarwinds.net/pub/SolarWinds-TFTP-Server.exe	TFTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sonic WALL[102]	Multiple	Content Filtering	A vulnerability exists because addresses are not sufficiently checked when requests are made, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Content Filtering Software Bypassing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[103]	Unix	Solaris 8.0, 8.0 _x86	A vulnerability exists in the Web-Based Enterprise Management (WBEM) component because some files are installed with insecure permissions, which could let a malicious user obtain sensitive information, launch a Denial of Service, or obtain elevated privileges.	Patches available at: http://sunsolve.sun.com Patch 109135-27, Patch 109134-27	Sun Solaris WBEM Insecure Permissions	Low/ Medium (Medium if sensitive informa-tion can be obtained or elevated privileges can be obtained)	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[104]	Unix	Solaris 8.0 _x86, 8.0	A Denial of Service vulnerability exists when certain flags are set in the 'kmem_flags' parameter.	Patches available at: http://sunsolve.sun.com/pub-cgi/ Sun Patch 108529-16, Sun Patch 108528-16	Sun Solaris 8 KMEM_FLAG Denial of Service	Low	Bug discussed in newsgroups and websites.

[99] interSEC Security Advisory, October 18, 2002.
[100] Bugtraq, October 24, 2002.
[101] iDEFENSE Security Advisory, 10.24.02, October 24, 2002.
[102] Bugtraq, October 29, 2002.
[103] Sun(sm) Alert Notification, 48320, October 29, 2002.
[104] Sun(sm) Alert Notification, 48067, October 31, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SuSE[105]	Unix	Linux 7.0-7.3, 8.0, 8.1	Two vulnerabilities exist: a vulnerability exists in the 'runlpr' utility when malicious strings are passed via the commandline which could allow a malicious user to execute arbitrary commands; and a vulnerability exists in the html2ps filter that is included in the lprng print system, which could let a remote malicious user execute arbitrary commands.	Patches available at: ftp://ftp.suse.com/pub/suse/	LPRNG Runlpr & html2ps Command Execution	High	Bug discussed in newsgroups and websites.
Virtual zone[106]	Windows	SmartMail Server 1.0 BETA 10	A Denial of Service vulnerability exists when a large amount of data is sent via TCP port 25 or 110.	No workaround or patch available at time of publishing.	SmartMail Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Virtual zone[107]	Windows	SmartMail Server 2.0	A Denial of Service vulnerability exists when a client is sending data and then closes the connection unexpectedly.	No workaround or patch available at time of publishing.	SmartMail Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
vpopmail-CGIApps[108]	Unix	vpopmail-CGIApps 0.2	Two vulnerabilities exist: a vulnerability exists in the 'vadddomain' command due to insufficient sanitization, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'vpasswd' command due to insufficient sanitization, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://diario.buscadoc.org/index.php?topic=Programas	vpopmail-CGIApps Insufficient Sanitization	**High**	Bug discussed in newsgroups and websites.
Working Resources Inc.[109]	Windows 98/2000	BadBlue 1.7 .0	A vulnerability exists because it is possible to construct a web request that will circumvent access control restrictions and access the contents of password protected files/folders, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BadBlue Access Control Circumvention	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[105] SuSE Security Announcement, SuSE-SA:2002:040, October 31, 2002.
[106] Bugtraq, October 31, 2002.
[107] Bugtraq, October 31, 2002.
[108] Centaura Technologies Security Research Lab Advisory, October 24, 2002.
[109] Securiteam, October 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
YaBB[110]	Windows, Unix	YaBB 1.40 1.41	A Cross-Site Scripting vulnerability exists in the forum login script due to improper filtering of HTML tags in the username and password fields, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	YaBB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit script has been published,

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between October 16 and October 31, 2002, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 20 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Script Description
October 31, 2002	**Smartdos.pl**	**Perl script that exploits the SmartMail Denial of Service vulnerability.**
October 31, 2002	**Smartmail_2_dos.pl**	**Perl script that exploits the SmartMail Denial of Service vulnerability.**
October 30, 2002	Vaccine.c	A program that removes the ELF infecting virus Linux.Jac.8759 from binary files and includes an infected file.
October 29, 2002	Cuts-0.01.tar.gz	CUTs (cellphone unix terminal) is a procmail hack that allows you to use a normal cellphone's messaging capability as a Unix/Linux terminal from anywhere.

[110] Bugtraq, October 18, 2002.

Date of Script (Reverse Chronological Order)	Script name	Script Description
October 24, 2002	**Swtftp-ex.pl**	**Perl script that exploits the TFTP Server Large UDP Packet Denial of Service vulnerability.**
October 24, 2002	Tunnelfinder.zip	A proxy checker that can display information from a list of proxies by searching for proxy servers that permit the CONNECT command allowing an end user to achieve a higher level of anonymity.
October 24, 2002	**Virgil.txt**	**Exploit examples for the Virgil CGI Scanner Remote Command Execution vulnerability.**
October 24, 2002	**Wc.tar.gz**	**Two modified versions of the Slapper worm exploit made user-friendlier with simple interaction to define what host and port will be hit with the exploit.**
October 22, 2002	Anhttpd141c_exploit.java	Exploit for the AN HTTPD Malformed SOCKS4 Buffer Overflow vulnerability.
October 22, 2002	Sendmail-8-11-X.C	Script which exploits the Sendmail 8.11.x linux/x86 root vulnerability.
October 21, 2002	L-zonealarm.c	Remote Denial of Service exploit for ZoneAlarm Pro 3.1.291 and 3.0.
October 21, 2002	Md5 checksum ntal-0.2.2.tar.gz	Network Traffic Analyzer (formerly known as sniffer) is designed to be an extremely powerful, configurable, and versatile tool for monitoring network traffic. It can be used as a plain sniffer, as a tool for accounting, dynamic firewall updates, and many more things. It features scripting support and an event-driven architecture.
October 21, 2002	N-stealth-3.5-b62.zip	A vulnerability assessment tool for Windows which scans webservers for bugs that allow attackers to gain access. Uses a database of 19,000 vulnerabilities and exploits.
October 21, 2002	Rpcap-devel-0.23.tar.gz	RPCAP is a Remote Packet Capture system that enables you to run a packet capture program (the server) on a target computer, which will sniff the network traffic on that system, and uplink the captured packets to another host (the client), where the captured packets can be processed, analyzed and archived .
October 20, 2002	Bop.pl	Perl script which exploits the PlanetDNS v1.14 remote buffer overflow vulnerability.
October 20, 2002	Bsd-ptrace.c	BSD ptrace shellcode which injects a bindcode into the ppid, useful for breaking chroot.
October 18, 2002	**Goodies.tar.gz**	**Script which exploits the Windows 2000 RPC Service Remote Denial of Service vulnerability.**
October 18, 2002	**Hack.asp**	**Exploit for the YaBB Cross-Site Scripting vulnerability.**
October 18, 2002	**Winnuke.c**	**Script which exploits the Windows 2000 RPC Service Remote Denial of Service vulnerability.**
October 16, 2002	Flawfinder-1.21.tar.gz	Flawfinder searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first.

Trends

- **Multiple Kerberos distributions contain a remotely exploitable buffer overflow in the Kerberos administration daemon, which could let a remote malicious user obtain root privileges. The CERT/CC has received reports that indicate that this vulnerability is being exploited. For more information, see "Bugs, Holes & Patches" Table and CERT Advisory, CERT® Advisory CA-2002-29, located at: http://www.cert.org/advisories/CA-2002-29.html.**
- **There have been a significant number of calls from customers concerned about a widespread e-mail that invites users to pick up an "E-Card" from a website called FriendGreetings.com. For more information, see http://www.sophos.com/virusinfo/articles/greetings.html.**

- **Firewalls and other systems that inspect FTP application layer traffic may not adequately maintain the state of FTP commands and responses. As a result, an attacker could establish arbitrary TCP connections to FTP servers or clients located behind a vulnerable firewall. For more information see Vulnerability Note VU#328867, located at: http://www.kb.cert.org/vuls/id/328867.**
- **The CERT/CC has received confirmation that some copies of the source code for the Sendmail package have been modified by an intruder to contain a Trojan horse. For more information, see "Bugs, Holes, & Patches Table" and CERT® Advisory CA-2002-28 located at: http://www.cert.org/advisories/CA-2002-28.html.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of an e-mail-borne worm known as W32.Bugbear or I-Worm.Tanatos. For more information, see NIPC Advisory 02-008, located at: http://www.nipc.gov/warnings/advisories/2002/02-008.htm and Virus Section.**
- **The National Infrastructure Protection Center (NIPC) has been coordinating with the anti-virus and security community on the life cycle of "Slapper," the OpenSSL/Apache worm and all its variants. For more information, see NIPC ASSESSMENT 02-003, located at: http://www.nipc.gov/warnings/assessments/2002/02-003.htm.**
- **The SANS Institute and the National Infrastructure Protection Center (NIPC) have updated the list containing the Twenty Most Critical Internet Security Vulnerabilities. This list is broken into two categories: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. For more detailed information, see: http://www.sans.org/top20.**
- **Web CGI exploits and Microsoft vulnerabilities continue to be two of the more frequent ways which external malicious sources conduct their probes in their attempt to gain access to networks.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Stable	January 2002
2	W32/Bugbear-A	Worm	Increase	September 2002
3	W32/Yaha	Worm	Slight Increase	February 2002
4	W32/Nimda-A-O	File, Worm	Slight Decrease	September 2001
5	Elkern	File Infector	Slight Decrease	October 2001
6	I-Worm.Magistr	File, Worm	Slight Increase	March 2001
7	I-Worm.Sircam	Worm	Slight Increase	July 2001
8	I-Worm.Hybris	File, Worm	Increase	November 2000
9	Funlove	File	Slight Increase	November 1999
10	JS/NoClose	Trojan	Slight Decrease	May 2002

Note: Virus reporting may be weeks behind the first discovery of infection. A total 201 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 374 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

PE_APPIX.A (Aliases: W32.Appix.Worm, W32.Appix.C.Worm) (File Infector Virus): This file infector virus propagates via e-mail and mIRC. It draws from the Windows address book, The Bat! address book, and other files on the system for its list of recipients. An e-mail message is sent that contains a subject with various text strings and the attachment also has various names. The e-mail message has a blank message body. This file infector worm infects .BAT, .COM, .EXE, .PIF and .SCR files. Its infection routine, however, results in either the overwriting or corruption of target files.

PE_APPIX.B (Aliases: W32.Appix.B.Worm, W32/Appix.b, I-Worm.Apbost, Win32/Apbost.A@mm) (File Infector Virus): This variant of PE_APPIX.A propagates copies of itself by mass-mailing copies of itself using its own SMTP (Simple Mail Transfer Protocol) engine. The subject and attachment of the e-mail that it sends out vary; by using its maliciousVisual Basic Script component, VBS_APPIX.A, which sends an e-mail containing this worm as attachment using MAPI (Messaging Application Programming Interface). However, VBS_APPIX.A fails to carry out this routine due to errors in its codes. It also sends a copy of itself to all Internet Relay Chat (mIRC) users who are in the same channel as the infected user; or by dropping a copy of itself in the KaZaA network shared folder, making it easily accessible to other KaZaA users. It does this by disguising as a key generator application. This malware also infects files with BAT, COM and EXE extension names by attaching its malicious code at the start of target files.

VBS.Legion@mm (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm that uses Microsoft Outlook MAPI to send itself to first 8,000 contacts in the Outlook Address Book. It also attempts to spread through the KaZaA file-sharing network and deletes some antiviral product files when it is executed. The e-mail has the following characteristics:

- Subject: Legion Game
- Attachment: Legion.vbs

VBS_LIFELESS.A (Aliases: VBS/Generic@MM, VBS.VBSWG.gen, I-Worm.Lee-based, VBS/Lee-based.gen*, VBS/VBSWG-2B, VBS/WBSWG.1525) (Visual Basic Script Worm): This nondestructive Visual Basic Script malware propagates via e-mail by sending copies of itself to all recipients found in the target user's Microsoft Outlook address book. The e-mail that it sends out has this format:

- Subject: Gift for you!
- Attachment: gift for you.html.vbs

This malware also spreads via Internet Relay Chat (IRC) channels and opens a certain Web site upon execution. It is related to the VBS_VBSWG.GEN family of malware.

VBS.Pocus (Aliases: VBS.WhyMe, VBS/Sucop, VBS/WhyHoPo) (Visual Basic Script Virus): This is a VB Script virus that infects .vbs files in the root of the C drive. It infects by prepending itself to .vbs files. Due to a bug in the virus, the infected .vbs files no longer work.

W32.Anel@mm (Win32 Worm): This is a mass-mailing worm that replicates as e-mail. It uses Microsoft Outlook to send itself to the contacts in the Outlook Address Book. The e-mail message has the following characteristics:

- Subject: Hehehehtetetete
- Message Body: Hello Buddy , Check the Attachment And Have Fun With that, Yoohooo.
- Attachment: Checkwin.exe

W32.Appix.D.Worm (Win32 Worm): This is a variant of W32.Appix.B.Worm. It prepends itself to .bat, .com, .cmd, .exe, scr, .pif, and .msi files in the root folder of drive C, and prepends itself to all .exe files in the Windows installation folder. It also attempts to prepend itself to open files. It infects .php, .phtml, and .php3 files in the current folder, the root of drive C, the Windows installation folder, and the Windows system folder by appending code that is designed to infect other .php, .phtml, and .php3 files. It downloads the W32.Appix.D.Worm to a client computer that visits an infected web site. The worm spreads itself through mIRC. Also, the worm uses the current e-mail program or its own SMTP engine to send itself to all contacts in the Windows Address Book and in The Bat! e-mail program's address book. The e-mail message may have a combination of various subjects and attachments. The worm tries to disable some programs by terminating the active processes and stopping the active services.

W32.Buzzard@mm (Win32 Worm): This is a mass-mailing worm that spreads by e-mail. It is a Visual Basic application and is packed with tElock and UPX. The e-mail will have a subject and an attachment name which are randomly chosen from predetermined lists.

W32.Gaze@mm (Aliases: Win32.Gaz, MSIL/Gaze@MM, I-Worm.Gaze) (Win32 Worm): This is a mass-mailing worm that replicates by e-mail. It uses Microsoft Outlook to send itself to the contacts in the Outlook Address Book. The worm requires that the .NET framework be installed in order to propagate. The e-mail message has the following characteristics:

- Subject: faze
- Attachment: Game.exe

W32.HLLW.Gaobot (Alias: W32/Gaobot.worm) (Win32 Worm): This is a worm that copies itself as %system%\Sysldr32.exe. It then connects to an IRC server and listens for commands. By default, the worm will connect on ports 6,667 and 9,900. Some of the commands that it supports include commands to spread itself, using popular file sharing programs such as KaZaA, Bearshare, and Grokster. It shares itself as various filenames. The worm also attempts to spread to all computers on the network, using a utility that connects to a remote computer on port 445, it copies the Woinggg.exe file across the network, and then executes it.

W32.HLLW.Loxar (Win32 Worm): This is a worm that spreads using the KaZaA peer-to-peer network. It is written in Delphi and packed by the tElock runtime packer. It copies itself to the root folder of all drives, and to the KaZaA shared folder, using a name chosen randomly from a list that the worm carries. On December 13, the worm might start Notepad and display a message in the window. The worm attempts to terminate the processes of a number of antiviral and firewall programs.

W32/Opaserv-C (Aliases: Opaserv-E, W32.Opaserv.Worm, WORM_OPASERV.E, Win32.Opaserv.E, W32/Opaserv.worm) (Win32 Worm): This is a variant of W32/Opaserv-A and is a worm that spreads via network shares. When executed, the worm will create a file called brasil.exe or brasil.pif in the Windows folder on the current drive. W32/Opaserv-C then adds one of the following registry entries to run itself when the system starts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Brasil = C:\WINDOWS\brasil.exe

or

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Brasil = C:\WINDOWS\brasil.pif

The worm attempts to copy itself to the Windows folder on networked computers with open shared drives. It then modifies the win.ini file on the remote machine to ensure the copied file will be run on system start. The worm also searches local IP addresses for open C: shares and attempts to copy itself to the Windows folder of the share. Once the local area network has been scanned, the worm will start performing the same search on the Internet starting at a randomly generated IP address. As a result anyone connected to the Internet who has file sharing enabled and who enables NETBIOS over TCP/IP is potentially vulnerable to this worm. W32/Opaserv-C also attempts to connect to a website that is currently unavailable. This attempted connection is most likely intended as a means of updating the worm executable. The following three non-viral files may be found in the root folder of infected systems:

- put.ini
- scrsin.dat
- scrsout.dat

W32/Opaserv-F (Aliases: Worm.Win32.Opasoft.a, W32.Opaserv.Worm, WORM_OPASERV.G, Win32.Opaserv.G, W32/Opaserv.worm) (Win32 Worm): This is a variant of W32/Opaserv-A and is a worm that spreads via network shares. When executed, the worm will create a file called marco!.scr in the Windows folder on the current drive. W32/Opaserv-F then adds the following registry entry to run itself when the system starts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\cronos = <windows folder>\marco!.scr

The worm attempts to copy itself to the Windows folder on networked computers with open shared drives. It then modifies the win.ini file on the remote machine to ensure the copied file will be run on system start. The worm also searches local IP addresses for open C: shares and attempts to copy itself to the Windows folder of the share. Once the local area network has been scanned, the worm will start performing the same search on the internet starting at a randomly generated IP address. As a result anyone connected to the internet who has file sharing enabled and who enables NETBIOS over TCP/IP is potentially vulnerable to this worm. W32/Opaserv-F also attempts to connect to a website that is currently unavailable. This attempted connection is most likely intended as a means of updating the worm executable. The following three non-viral files may be found in the root folder of infected systems:

- tmp.ini
- scrsin.dat
- scrsout.dat

VBS.Likun@mm (Visual Basic Script Worm): This is a mass-mailing worm that replicates by e-mail. It uses Microsoft Outlook to send itself to the contacts in the Outlook Address Book. The e-mail message has the following characteristics:

- Subject: New Tool !
- Message Body: This tool can speed up your PC up to 15% !
- Attachment: (The file name of the script.)

When VBS.Likun@mm runs, it copies itself as %windir%\Xp32dll.vbs. The worm creates the value, “lehota %windir%\xp32dll.vbs,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the worm starts when you start or restart Windows.

W32/Ramidle (Win32 Virus): If executed, W32/Ramidle is a file infector infecting all files in the same directory in which it is run with the following extensions: *.exe, *.scr, *.cpl . It will also delete the following files:

- C:\Windows\Asd.exe
- C:\Windows\Calc.exe
- C:\Windows\Notepad.exe
- C:\Windows\Pbrush.exe
- C:\Windows\Cdplayer.exe

Finally, on the 7th, 12th, 17th, and 22nd of each month, it will drop the file "ramlide.bmp" as the infected users desktop wallpaper.

W32.Wonna@mm (Win32 Worm): This is a mass-mailing worm that sends itself to all contacts in the Microsoft Outlook Address Book. The e-mail message has many different subject lines and many different attachment names. The worm also spreads by using the KaZaA file-sharing program. It attempts to trick users into downloading and executing the worm. If you use mIRC, the worm sends itself to other mIRC users.

VBS.Zsyang@m (Visual Basic Script Worm): VBS.Zsyang@m is a worm that replicates by e-mail. It uses Microsoft Outlook to send itself to the first contact in the Outlook Address Book. The e-mail message has the following characteristics:

- Subject: Edit11
- Message Body: Edit13
- Attachment: Zsy.vbe

W95.Sleepyhead.5632 (Aliases: W32.Sleepyhead, W95.Sleepyhead) (Win32 Virus): This is a virus that infects Portable Executable (PE) files under Windows 95/98/ME. When an infected file is executed, it searches memory for Kernel32.dll functions and then it loads User32.dll and WSock32.dll libraries and searches for functions in them. After that, the virus searches through all folders and subfolders on all hard drives and mapped drives, beginning at the root. It appends itself to the end of the host file image and infects only those PE files that have an .exe file extension and are not already infected by the same virus. Infected files grow in size by 5,632 Bytes and their time and date stamp also change to the time of infection. W95.Sleepyhead.5632 does not display any messages or produce any malicious side effects. The virus periodically searches for all mapped drives one-by-one in a separate search thread and starts finding files to be infected. It infects files very slowly and is almost unnoticed. When a new file is infected, it waits 15 seconds before trying to infect another one. It marks a byte in the header of infected files so that it does not reinfect them later. Every now and then when an infected file is executed, the virus tries to drop itself as the pure dropper file %windir%\System\Winword.exe. This file cannot be repaired. The virus may corrupt PE files that have appended data such as self-extracting archives. These bytes cannot be restored. This is because the virus only checks the image size in the PE file header and does not check whether there is already appended data present. In these situations it corrupts the first 5,632 bytes in that appended section.

W97M.Courage.C (Alias: Macro.Word97.Courage) (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents when you open them. It infects by using the Normal.dot template and active documents. The virus consists of three modules:

- AUTOOPEN
- AUTONEW
- AUTOEXEC

On the 15th every month, the virus displays a message in Chinese.

W97M.Wisefool (Word 97 Macro Virus): W97M.Wisefool is a polymorphic macro virus that infects Microsoft Word documents when you open them. It is a macro virus that infects Microsoft Word documents. It spreads from infected documents to the Normal.dot template, which then infects documents when you open them. The macro is polymorphic in that it changes the names of its modules and variables to random alphanumeric strings. As a result, these values will change from infection to infection. There is no other payload.

WORM_DUKSTEN.B (Aliases: W32/BogusBear.A, WORM_BOGUSBEAR.A, W32.Duksten.B@mm, W32.Protex.Worm) (Internet Worm): This worm propagates via e-mail by sending a copy of itself attached to messages with the following details:

- From: Alerta_RaPida &ltboletin@viralert.net>
- Subject: ProTeccion TOTAL contra W32/Bugbear (30dias)
- Attachment: PROTECT.ZIP

If the system indicates that the year is 2003, this worm causes Windows to exit. And if it has already altered the registry, the system is prevented from subsequently starting up in Windows.

WORM_MERKUR.A (Alias: W32.HLLW.Merkur@mm, Win32.Merkur.A, W32/Merkur@MM) (Win32 Worm): This memory-resident worm propagates via e-mail, the KaZaA file-sharing utility, and mIRC. It uses Microsoft Outlook to send e-mail with the following details:

- Subject: Update your Anti-virus Software
- Attachment: TASKMAN.EXE

It drops an IRC script component that configures mIRC so that the Internet Relay Chat client sends a copy of this worm to other chat users. This worm also drops a batch file component that deletes .JPG, .MPG, .BMP, and .AVI files from certain directories.

WORM_PORKIS.B (Internet Worm): This worm is a variant of WORM_PORKIS.A. It spreads via e-mail by sending itself to all recipients listed in the Windows Address Book (WAB). The details of the e-mail that it sends out are as follows:

- To: <Undisclosed-Recipient:;>
- Subject: Bin Laden Bastardo!!!!!
  Leggete urgentemente questa e-mail!!
  (11 settembre da ricordare)
  Verit
- Attachments:jocker.exe, Joker.exe, Jok.exe

WORM_SPONGE.A (Alias: W32/Sponge@MM) (Internet Worm): This destructive, memory-resident worm propagates via Microsoft Outlook by sending itself as an e-mail attachment to all addresses found in the Microsoft Outlook address book. It arrives in an e-mail with the following details:

- Subject: SpongeBob Wallpaper
- Message Body: Send this to your friends and make them laugh…
- Attachment: Spongy.exe

The worm also overwrites .SCR and .PIF files and infects Microsoft Word documents by overwriting the NORMAL.DOT template.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AIM-Flood	N/A	CyberNotes-2002-16
Arial	N/A	CyberNotes-2002-08
Backdoor.AIMVision	N/A	CyberNotes-2002-21
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12

Trojan	Version	CyberNotes Issue #
Backdoor.AntiLam.20	20	CyberNotes-2002-18
Backdoor.Armageddon.B	N/A	CyberNotes-2002-20
Backdoor.Asniffer	N/A	CyberNotes-2002-21
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	N/A	CyberNotes-2002-18
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	N/A	CyberNotes-2002-18
Backdoor.DarkFtp	N/A	CyberNotes-2002-19
Backdoor.DarkSky.B	B	CyberNotes-2002-20
Backdoor.DarkSky.C	C	CyberNotes-2002-21
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Delf.D	**D**	**Current Issue**
Backdoor.Dindang	**N/A**	**Current Issue**
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.Elitem	N/A	CyberNotes-2002-20
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	N/A	CyberNotes-2002-18
Backdoor.Feardoor	N/A	CyberNotes-2002-21
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Ana	N/A	CyberNotes-2002-20
Backdoor.FTP_Ana.B	B	CyberNotes-2002-20
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.FunFactory	N/A	CyberNotes-2002-19
Backdoor.Goster	N/A	CyberNotes-2002-20
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.GWGhost	N/A	CyberNotes-2002-21
Backdoor.Helios	N/A	CyberNotes-2002-19
Backdoor.Hupigeon	N/A	CyberNotes-2002-21
Backdoor.Kaitex.B	N/A	CyberNotes-2002-20
Backdoor.Kaitex.C	**C**	**Current Issue**
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Klb	**N/A**	**Current Issue**
Backdoor.Kryost	N/A	CyberNotes-2002-18
Backdoor.Laphex	N/A	CyberNotes-2002-18
Backdoor.Laphex.Client	N/A	CyberNotes-2002-18
Backdoor.Lastdoor	N/A	CyberNotes-2002-18
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	B	CyberNotes-2002-18
Backdoor.Litmus.203.b	**B**	**Current Issue**
Backdoor.Litmus.2a	2a	CyberNotes-2002-20
Backdoor.LittleWitch.B	**B**	**Current Issue**
Backdoor.Miffice	N/A	CyberNotes-2002-18
Backdoor.Mirab	N/A	CyberNotes-2002-13

Trojan	Version	CyberNotes Issue #
Backdoor.Mite	N/A	CyberNotes-2002-18
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.Niovadoor	**N/A**	**Current Issue**
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.Optix.04	04	CyberNotes-2002-19
Backdoor.Optix.04.b	**B**	**Current Issue**
Backdoor.Optix.04.c	**C**	**Current Issue**
Backdoor.OptixPro.10	10	CyberNotes-2002-18
Backdoor.OptixPro.11	11	CyberNotes-2002-20
Backdoor.OptixPro.11.b	**B**	**Current Issue**
Backdoor.OptixPro.12	12	CyberNotes-2002-18
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Pest.Cli	N/A	CyberNotes-2002-20
Backdoor.Pestdoor	N/A	CyberNotes-2002-20
Backdoor.Phoenix	N/A	CyberNotes-2002-19
Backdoor.Platrash	N/A	CyberNotes-2002-21
Backdoor.Ptakks.B	N/A	CyberNotes-2002-18
Backdoor.RCServ	N/A	CyberNotes-2002-19
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Revrs	**N/A**	**Current Issue**
Backdoor.RMFDoor.Cli	N/A	CyberNotes-2002-20
Backdoor.Robi	N/A	CyberNotes-2002-18
Backdoor.Roxrat.10	N/A	CyberNotes-2002-20
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Sdbot.B	**B**	**Current Issue**
Backdoor.Seamy	N/A	CyberNotes-2002-18
Backdoor.Singu	**N/A**	**Current Issue**
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Sparta.B	B	CyberNotes-2002-19
Backdoor.Sparta.C	C	CyberNotes-2002-21
Backdoor.Spigot.B	**B**	**Current Issue**
Backdoor.Synrg	**N/A**	**Current Issue**
Backdoor.Tela	N/A	CyberNotes-2002-17
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Theef.B	B	CyberNotes-2002-21
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Wiween	**N/A**	**Current Issue**
Backdoor.Wold	**N/A**	**Current Issue**
Backdoor.Y3KRat.15	N/A	CyberNotes-2002-17
Backdoor.Zenmaster	N/A	CyberNotes-2002-19
Backdoor-AKO	N/A	CyberNotes-2002-20
BackDoor-AKR	N/A	CyberNotes-2002-19

Trojan	Version	CyberNotes Issue #
BackDoor-ALT	N/A	CyberNotes-2002-21
BackDoor-AMB	**N/A**	**Current Issue**
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/EHKSLogger	N/A	CyberNotes-2002-19
BDS/Pestdoor.4	N/A	CyberNotes-2002-20
BDS/Sporkbot	N/A	CyberNotes-2002-20
BDS/WinSpyer	**N/A**	**Current Issue**
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
Bneo.Trojan	N/A	CyberNotes-2002-18
Cardst	N/A	CyberNotes-2002-17
Cytron	N/A	CyberNotes-2002-20
Dewin	N/A	CyberNotes-2002-08
Downloader-W	N/A	CyberNotes-2002-08
FakeGina.Trojan	N/A	CyberNotes-2002-16
Fortnight	N/A	CyberNotes-2002-10
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
IRC-Smev	N/A	CyberNotes-2002-08
Jekord	N/A	CyberNotes-2002-19
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
Netbus.160.Dropper	N/A	CyberNotes-2002-17
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNCrack	N/A	CyberNotes-2002-18
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16
PWSteal.BStroj	N/A	CyberNotes-2002-20
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17
PWSteal.SoapSpy	N/A	CyberNotes-2002-18
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
Reboot-R	N/A	CyberNotes-2002-18
StartPage-B	N/A	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/EvilDX	N/A	CyberNotes-2002-19
Tr/SCKeyLog.Spy.20	**N/A**	**Current Issue**
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/WLoader	N/A	CyberNotes-2002-20
TR/Zirko	N/A	CyberNotes-2002-10

Trojan	Version	CyberNotes Issue #
Trj/GhostGirl	N/A	CyberNotes-2002-19
Troj/Apher-A	N/A	CyberNotes-2002-17
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/FireAnv-A	N/A	CyberNotes-2002-19
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Netdex-A	N/A	CyberNotes-2002-21
Troj/Nethief-C	**N/A**	**Current Issue**
Troj/Ritter-A	N/A	CyberNotes-2002-17
Troj/Tobizan-A	N/A	CyberNotes-2002-16
Troj/Unreal-A	N/A	CyberNotes-2002-16
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMBNUKE.A	N/A	CyberNotes-2002-18
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_SUOMIA.A	N/A	CyberNotes-2002-18
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Adclicker	N/A	CyberNotes-2002-19
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.Avid	N/A	CyberNotes-2002-19
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	N/A	CyberNotes-2002-18
Trojan.Diskfil	N/A	CyberNotes-2002-19
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Iblis	**N/A**	**Current Issue**
Trojan.IrcBounce	N/A	CyberNotes-2002-19
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Lovead	N/A	CyberNotes-2002-19
Trojan.Nullbot	N/A	CyberNotes-2002-19
Trojan.Portacopo:br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.Ajim_bbs	N/A	CyberNotes-2002-19
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.PWS.QQPass.C	N/A	CyberNotes-2002-21
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.Win32.Filecoder	N/A	CyberNotes-2002-18
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
Trojan.WinReboot	N/A	CyberNotes-2002-20
UNIX_ALUTAPS.A	N/A	CyberNotes-2002-21
VBS.AVFake	**N/A**	**Current Issue**
VBS.Krim.C	**N/A**	**Current Issue**
VBS.Lavra.B.Worm	N/A	CyberNotes-2002-19

Trojan	Version	CyberNotes Issue #
VBS.Zevach	N/A	CyberNotes-2002-15
VBS/Helvis	**N/A**	**Current Issue**
VBS_CHICK.B	N/A	CyberNotes-2002-07
W32.Azak	N/A	CyberNotes-2002-16
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16
W32.Kotef	N/A	CyberNotes-2002-16
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.STD.D	**N/A**	**Current Issue**
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15
Worm/Garra	N/A	CyberNotes-2002-20

Backdoor.Delf.D (Aliases: Backdoor.Delf.bd, BackDoor-ADX): This is a backdoor Trojan that gives an attacker unauthorized access to a compromised computer. This backdoor has the ability to log keystrokes. The presence of the file Xdaemon.exe is an indicator of a possible infection. Backdoor.Delf.D is a Delphi application, and is packed with UPX. It is a variant of Backdoor.Delf. When Backdoor.Delf.D runs, it displays the message:

- setup failed

and then copies itself as %windir%\Xdaemon.exe. The Trojan creates the value, "Microsoft xdaemon 2.0 %windir%\xdaemon.exe –disable," in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. The Trojan installs hook procedures into a hook chain to monitor the system for any keyboard and mouse input. The keyboard and mouse hook procedure processes the keystrokes or mouse actions and pass the hook information to the next hook procedure in the current hook chain. This permits Backdoor.Delf.D to intercept any keystrokes. The Trojan notifies the client side using ICQ pager. Once installed, Backdoor.Delf.D waits for commands from the remote client.

Backdoor.Dindang (Aliases: Backdoor.Dindang, Backdoor-ALQ, BKDR_DINDANG.A): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. The existence of the file Vmisd.dll is a possible sign of infection. When Backdoor.Dindang runs, it creates the file %system%\Vmisd.dll. The Trojan uses this file to store internal configuration data. This file is not malicious. The Trojan creates the value, "<Trojan file name without extension> <Trojan full path and file name with extension>," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. After Backdoor.Dindang is installed, it waits for the commands from the remote client.

Backdoor.Kaitex.C: This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. It is a variant of Backdoor.Kaitex. When Backdoor.Kaitex.C runs, it creates the value, "Service [path to the Trojan]," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process to continue to run after you log off. In this case, Backdoor.Kaitex.C closes only when you shut down the system. The Trojan notifies the client side using ICQ pager. After Backdoor.Kaitex.C is installed, it waits for commands from the remote client. The commands allow the malicious user to perform the following actions:

- Download and execute files
- Alter system parameters, such as screen resolution and system colors
- Perform Denial of Service (DoS) attacks

Backdoor.Klb: This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. Client and the server versions of this Trojan exist; both are detected as Backdoor.Klb. The client version of this Trojan is used by a malicious user to access a computer after the server version has been executed on the infected system. The malicious user can then use the upload command on the client to upload any executable to the infected system and then run it. The client can also be used to create UPX-packed server versions of this Trojan. These server versions can use any port number and can have any file name. The server is used to open a port and listen for a connection from the client. When the Backdoor.Klb server runs, it copies itself to the %windir% folder. The file name can be any name of the malicious user's choice; it has the .exe extension. Backdoor.Klb adds the value, "<any file name> %windir%\<any file name>.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Backdoor.Litmus.203.b (Aliases: Backdoor.Litmus.203, BackDoor-JZ): This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. The malicious user can control the system via commands issued through IRC. Backdoor.Litmus.203.b is a variant of Backdoor.Litmus.203. When Backdoor.Litmus.203.b runs, it copies itself as %windir%\Random\Svchost.exe. The Trojan creates the value, "LTM2   %windir%\Random\Svchost.exe," in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. The Trojan connects to an IRC server using port 6667, joins a specific channel, and notifies a malicious user by sending a private message. It then waits for the commands that the malicious user transmits using IRC.

Backdoor.LittleWitch.B (Aliases: Backdoor.LittleWitch.61.b, New BackDoor1): This is a backdoor Trojan that gives an attacker unauthorized access to a compromised computer. The presence of the file Rundll.exe is an indicator of a possible infection. By default, it opens port 31,320 on the compromised computer. Backdoor.LittleWitch.B is a Delphi application, and is packed with UPX. When Backdoor.LittleWitch.B runs, it copies itself as %system%\Rundll.exe. It creates the file %windir%\Usr.dat. This file stores passwords in an encoded form. The Trojan creates the value, "Rundll Rundll.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. If the operating system is Windows 95/98/ME, Backdoor.LittleWitch.B attempts to obtain access to the password cache that is stored on the local computer. The cached passwords include modem and dialup passwords, URL passwords, share passwords, and others. The Trojan notifies the client side using ICQ pager. Once installed, Backdoor.LittleWitch.B waits for commands from the remote client. The dialog between Backdoor.LittleWitch.B and the connected client uses messages that are in Spanish.

Backdoor.Niovadoor (Alias: Backdoor.Niovadoor.10): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 54312 on the infected computer. The Trojan attempts to disable some antiviral and firewall programs by terminating their active processes. When Backdoor.Niovadoor runs, it displays this message:

- A General Fault Error has Occurred in Address: 27x334F

It copies itself as %system% \PIDLex.exe. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process to continue to run after the user logs off. In this case, Backdoor.Niovadoor will close only when the system is shut down. In addition, Backdoor.Niovadoor attempts to obtain an access to the password cache that is stored on the local computer. The cached passwords include modem and dial-up passwords, URL passwords, share passwords, and others. The Trojan intercepts confidential information by hooking keystrokes. This permits Backdoor.Niovadoor to steal confidential messages that are typed on an infected computer. The Trojan uses ICQ pager to notify the client side. After Backdoor.Niovadoor is installed, it waits for commands from the remote client.

Backdoor.Optix.04.b (Alias: Backdoor.Optix.50): This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 5151 on the compromised computer. Backdoor.Optix.04.b is a variant of Backdoor.Optix.04. When Backdoor.Optix.04.b runs, it displays this message:

- missing blocker.dll is not currently registered

It copies itself as %system%\Msdodi.exe. The Trojan creates the value, "winhelperapp %system%\msdodi.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. After Backdoor.Optix.04.b is installed, it waits for commands from the remote client.

Backdoor.Optix.04.c (Alias: Backdoor.Optix.50): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 5151. Backdoor.Optix.04.c is a variant of Backdoor.Optix.04. When Backdoor.Optix.04.c runs, it copies itself as "windir%\olefiles\Winupdtr.exe." The Trojan creates the value, "Common Startup %windir%\olefiles," in the registry key

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

so that the Trojan runs each time that you starts Windows. After Backdoor.Optix.04.c is installed, it waits for the commands from the remote client. The commands allow the malicious user to perform the following actions:

- Deliver system and network information, including login names and cached network passwords, to the malicious user.
- Manage the installation of the Trojan.
- Download and execute files.

Backdoor.OptixPro.11.b: This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 1337 on the infected computer. Backdoor.OptixPro.11.b is a variant of Backdoor.OptixPro.11. When Backdoor.OptixPro.11.b runs, it displays this message:

- General Protection Fault at address 0x00000004

It copies itself as %windir%\Spooll32.exe. The Trojan creates the value, "vscanner %windows%\spooll32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. It attempts to disable some antiviral and firewall programs by terminating their active processes. It installs hook procedures into a hook chain to monitor the system for keyboard and mouse messages. The keyboard and mouse hook procedure process the messages and pass the hook information to the next hook procedure in the current hook chain. This permits Backdoor.OptixPro.11.b to intercept keystrokes. The Trojan notifies the client side through e-mail. After Backdoor.OptixPro.11.b is installed, it waits for commands from the remote client.

Backdoor.Revrs (Alias: Backdoor.ReverseTrojan.211): This Trojan allows unauthorized access to the infected computer. It also attempts to update itself over the Internet. When the Trojan runs, it copies itself as %windir%\System\Msgsrv16.exe and %windir%\System\Directx3d.exe. Next, the Trojan adds the value, "Service386Shell %windir%\System\msgsrv16.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

and the value, "DirectX 3D Service %windir%\System\DirectX3D.exe," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. After a connection is established, the malicious user can do the following:

- Download and upload files
- Delete files
- Execute files
- Restart Windows
- Close windows
- Display messages
- Open and close the CD-ROM tray
- Log keystrokes
- Steal AOL Instant Messenger, ICQ, or MSN Messenger user name and password information

Backdoor.Sdbot.B (Aliases: Backdoor.IRC.SdBot.gen, IRC-Sdbot): This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. The malicious user can control the system via commands issued through IRC. Backdoor.Sdbot.B is a variant of Backdoor.Sdbot. When Backdoor.Sdbot.B runs, it copies itself as %system%\Syscfg32.exe. The Trojan creates the value, "Configuration Loader   syscfg32.exe," in these registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

so that the Trojan starts when you start or restart Windows. The Trojan connects to an IRC server using port 6667, joins a specific channel, and notifies a malicious user by sending a private message. It then waits for commands that the malicious user transmits using IRC.

Backdoor.Singu (Alias: Backdoor.Singu.g): This Trojan allows unauthorized access to the infected computer. It also attempts to update itself over the Internet. It is written in the Delphi programming language and packed with UPX. By default it opens port 2002. When the Trojan runs, it copies itself as %windir%\Services.exe. Next, the Trojan adds the value, "winlogon %windir%\services.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It creates the file %windir%\Winservices.dll. This is the configuration file for the Trojan.

Backdoor.Spigot.B (Aliases: Backdoor.G_Spot.20, BackDoor-AAG): This is a Backdoor Trojan that gives an attacker unauthorized access to a compromised computer. The presence of the file GSpot.exe is an indication of infection. Backdoor.Spigot.B is a Delphi application, packed with UPX. Backdoor.Spigot.B is a variant of Backdoor.Spigot. When the Trojan runs, it displays this message:

- Runtime error 216 at 0040525F

It copies itself as %system%\GSpot.exe. The Trojan creates the value, "WindowsUpdater %system%\GSpot.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. The Trojan notifies the client side using ICQ pager. Once installed, Backdoor.Spigot.B waits for commands from the remote client

Backdoor.Synrg (Alias: Troj/Synrg-A): This Trojan allows unauthorized access to the infected computer. It attempts to update itself over the Internet and spread itself using mIRC. The Trojan uses HTTP port 80 and various IRC ports to communicate. When the Trojan runs, it copies itself as %windir%\System\Winregsrv.exe. It also creates the following files in the %windir%\System folder:

- Info
- Nicklist.txt
- Updater.exe
- Winsck.ocs
- Msinet.ocx

The first three files are associated with the Trojan's mIRC and update functions. Next, the Trojan adds the value, "winregsrv %windir%\system\winregsvr.exe" to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows.

Backdoor.Wiween: Backdoor.Wiween is a Linux ELF executable wrapped using the Burneye obfuscation and encryption tool. It poses as an exploit against the Linux TCP/IP stack. This appears to be an attempt to fool would-be Linux malicious users into running this Trojan on their own systems. The executable is password-protected and will not run unless the proper password is provided. When the proper password is entered, Backdoor.Wiween first checks that it is being run as the root user and with at least one command-line argument. If these conditions are met, it performs the following actions:

- It simulates the execution of an exploit by printing bogus information to the terminal.
- It attempts to send the network configuration and shadow password file of the local machine to three e-mail addresses on the Internet.
- It opens a TCP port above 4000 and provides a root shell to any attacker who connects to the port.

When Backdoor.Wiween runs, the first line that it displays is, "McKenzy Wihle GSH security - 9/01/02:" When it mails the system information, Backdoor.Wiween creates a script under /tmp/.tmpkern1. Backdoor.Wiween intends to delete this file, but due to a bug, the file remains on the system after the backdoor has finished executing.

Backdoor.Wold: This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. The Trojan modifies the system to execute itself at startup and additionally upon execution of ICQ. The existence of the file "Dimitris World.exe" is an indicator of a possible infection.

BackDoor-AMB: This is a remote access Trojan. It uses Microsoft MSN Messenger to access victim machines. There are several variants of the trojan. One variant of the trojan copies itself to Windows directory as "Windll32.dll," and sets the following registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  "Windll32" = C:\WINDOWS\Windll32.exe"

It also changes the start page of Internet Explorer. Other variants do not make these changes. When run, the trojan launches the MSN Messenger executable in the background, and listens for various commands. Malicious users can use MSN Messenger from another machine to send commands to victim's machine.

BDS/WinSpyer: This Trojan could potentially allow unauthorized key strokes to be logged and used for malicious intent (i.e. containing passwords, credit card information, etc.). If executed, the keylogger copies itself to the \windows\%system\ directory under the filename, "Spy.exe." It also creates the file "Spy.txt" (contains the logged keystrokes) in the \windows\%system% directory. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  "SPY"="C:\\WINDOWS\\system\\SPY.EXE"

Tr/SCKeyLog.Spy.20: This Trojan could potentially allow unauthorized key strokes to be logged and used for malicious intent (i.e. containing passwords, credit card information, etc.). If keylogger generator is used, it will create a new keylogging Trojan with the following details:

- Name: <Random>.exe
- Length: ~33KB

The keylogger copies itself to the \windows\%system\ directory under a random filename with the file extension .exe (i.e. ntvdscm.exe) and under the random filename ending with the extension .dll (i.e. ntvdscm.dll). The filename of the .exe file and the .dll will always match. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "ntvdscm"="C:\\WINDOWS\\SYSTEM\\ntvdscm.exe"

Troj/Nethief-C (Aliases: Backdoor.Nethief.XP.c, BackDoor-TW Trojan, Backdoor.NetThief, BDS/Nethief.XP.C, Backdoor.Win32.Nethief.80384): This is a backdoor Trojan that copies itself to IExplorer.exe in the Windows system folder and sets the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Internet Explorer = Iexplorer.exe

Trojan.Iblis (Alias: Backdoor.Iblisdoor.02): This is an IRC Bot program that performs nuisance activities against other users of IRC who are logged into the same server as the IRC Bot program.

VBS.AVFake (Alias: Trojan.VBS.Carewmr): This Trojan is written in Visual Basic Script and attempts to delete registry values for several antiviral and firewall products. VBS.AVFake attempts to fool you into thinking that it is an antiviral program. On September 1 it displays the message, "Mr.Carew vuelve otra vez!!, jaja." The destructive portion of the payload attempts to delete C:\Windows. This is hard-coded and not dependent on system variables. It attempts to delete these values:

- SystemTray
- AVPCC
- NAVW32
- TrueVector
- ZoneAlarm Pro

from the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

The script creates the following folders:

- C:\Symantec
- C:\KasperskyLabs
- C:\PandaSoftware
- C:\TrendMicro
- C:\Eset-Nod-f---ed (Censored for this write-up)

It also drops a variety of files in the root of drive C.

VBS/Helvis: When executed, the Trojan will modify the registry setting by setting the value to 0:

- HKEY_CURRENT_USER\Software\MicrosoftWindows Scripting Host\Settings\Timeout,"0"

The Trojan will then open up the website www.madblast.com using Internet Explorer and a picture of an Elvis impersonator will be displayed. Using Outlook, the Trojan will e-mail all messages found in the Inbox and Sent Items to the e-mail address vcheckpr@hotmail.com. Messages found in Inbox will be sent to the above address with the subject line modified with the string "ibox" and the count number. Messages found in Sent Items will be sent to the above address with the subject line modified with the string "sbox" and the count number. All messages that contain Halloween Elvis in the subject line will be deleted. The Trojan will create another file VirusChecker.vbs in the hard coded path: c:\winnt\profiles\all users\start menu\programs\startup\. This file will also send messages found in the Inbox and Sent mail folders that have been received or sent the day before with the exception of Monday as it will send the messages that are three days old.

VBS.Krim.C: VBS.Krim.C copies itself as Valentina.jpg.vbs to all logical and network drives, including drive A. The Trojan Horse/worm also spreads through IRC as Valentina.htm. This worm has three payloads, one of which formats drive C if the right condition is met.

W32.STD.D (Alias: W32/STD.d.worm): W32.STD.D attempts to send a copy of itself to other mIRC users. Two variants of W32.STD.D have been found. Both Trojans have bugs and do not spread through mIRC. This threat is written in the Microsoft Visual Basic programming language. W32.STD.D deletes .dat files in the C:\Program Files\Norton AntiVirus folder.